FORTINET

Release Notes

FortiSwitchOS 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 22, 2022
FortiSwitchOS 7.2.0 Release Notes
11-720-774533-20220822

TABLE OF CONTENTS

Change log

Date	Change Description
April 13, 2022	Initial release for FortiSwitchOS 7.2.0
April 14, 2022	• Updated the “What’s new in FortiSwitchOS 7.2.0” section. • Updated the “By default, auto-network is enabled in FortiSwitchOS 7.2.0” section. • Removed bug 784742 from “Known issues.” • Added bug 659487.
April 16, 2022	Updated the “What’s new in FortiSwitchOS 7.2.0” section.
April 22, 2022	Updated the “What’s new in FortiSwitchOS 7.2.0” section.
April 25, 2022	Added bug 802786 as a known issue.
April 26, 2022	Removed the “Upgrading from FortiSwitchOS 6.x or 7.0 to FortiSwitchOS 7.2.0” section.
June 13, 2022	Added bug 667079 as a known issue.
July 19, 2022	Added the removal of `switch-mgmt-mode` to the “What’s new in FortiSwitchOS 7.2.0” section.
August 22, 2022	Changed the description of bug 659487.

Introduction

This document provides the following information for FortiSwitchOS 7.2.0 build 0393.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.0 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.2.0

Release 7.2.0 provides the following new features:

- You can now configure in the CLI whether packets with specific source static MAC address are allowed or dropped. By default, they are allowed.
- You can now send Wake-on-LAN (WoL) "magic" packets from a system interface or switch port to a specific MAC address.
- You can now use CLI commands to run REST API requests locally.
- VXLAN tunnels are now supported.
- You can now use the CLI for multiple path traceroute, which allows you to find all the routers that perform load balancing between the FortiSwitch unit and destination.
- The `execute restore` and `execute backup` commands now support IPv6 addresses.
- You can now configure an IPv6 address and netmask with correction for the administrative distance in the Border Gateway Protocol version-4 (BGP-4) routing parameters.
- The Operation pane of the *System* > *Dashboard* page now displays the status of the power supply units (PSUs) with indicator lights to allow administrators to quickly identify any problems. The PSU status is shown only on FortiSwitch models with redundant PSUs.
- You can now configure an automation stitch by specifying a trigger and the action to be performed. The automation stitch can be triggered by configuration changes, switch reboots, logged events, and scheduled times. The triggered action can be running a CLI script, sending an email message, displaying an alert in the console, or generating an SNMP trap.
- The `diagnose debug application alertd` command now also reports measurements from the CPU, memory, and disk sensors.
- You can now count ingress and egress packets by color in the GUI and CLI:
  - Ingress packets are marked green if the traffic rate is within the guaranteed information rate. Ingress packets are marked yellow if they exceed the committed burst size but do not exceed the excess burst size. All other ingress packets are marked red.
  - Egress packets are marked green if the traffic rate is within the guaranteed information rate. All other egress packets are marked yellow.
- IPv6 addresses are now supported when modifying the administrative distance for Border Gateway Protocol version-4 (BGP-4) routing parameters.
- IPv6 addresses are now supported when configuring a link probe and viewing the link monitor in the GUI.
- You can now select whether to advertise the IPv4 management address, the IPv6 management address, or no management address in the Management Address TLV. By default, both IPv4 and IPv6 addresses are advertised.
- The VLAN name TLV is now supported in the LLDP profile. When this TLV is enabled, the specified VLAN names are advertised in LLDP.
- You can now configure a physical port or trunk as a routed VLAN interface (RVI) for layer-3 routing protocols.
- You can now configure an IGMP static group to ignore dynamic joins from other ports. Preventing other ports from joining means that administrators control which ports receive traffic. This option is available in the GUI and CLI; it is disabled by default, which allows other ports to dynamically join.
- You can now configure an MLD static group to ignore requests from other ports to become members. Preventing other ports from joining means that administrators control which ports receive traffic. This option is available in the CLI; it is disabled by default, which allows other ports to dynamically join.
- The new `diagnose sys permission {list | list-by-accprofile | list-cli}` commands list the access permissions for access profile groups, access profiles, and CLI paths.

- You can now configure virtual routing and forwarding in the FortiSwitchOS GUI.
- Partial VLAN mapping is now supported by the FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, FS-148F-FPOE, and FSR-112D-POE models.
- You can now configure an SNMP trap so that you receive a message when a layer-2 MAC address has been added, deleted, or moved.
- As part of the existing support for RFC 1493, the following OID has been added:

Name	OID
dot1dStaticTable	1.3.6.1.2.1.17.5.1

- The new `diagnose sys remote assistance` commands allow Customer Support (ETAC) to examine your FortiSwitch unit remotely to gather more data about your switch's configuration and to find the solution to your issue. The remote assistance session uses an SSL tunnel for a secure connection. When the remote assistance session is active, it is shown in the *System Information* panel of your FortiSwitch dashboard, and a warning against local changes is displayed at the top of the GUI.
- You can now use the `config log disk filter` and `config log disk setting` commands to save event log messages in flash memory.
- The following statistics for the flash partitions are now displayed on the *System* > *Config* > *Firmware* page:
  - Content of each partition
  - Total size of the partition
  - How much of the partition is used
  - Percent used
  - Status
  - Which image will be loaded when the FortiSwitch unit is restarted
- You can now generate a detailed debugging report from the *System* > *Debug Report* page and then download it so that you can send it to technical support. The report is identical to the output of the `diagnose debug report` command.
- A new *Switch* > *DHCP Snooping* page allows you to enable the trusted DHCP server list for DHCP snooping.
- You can now configure the maximum burst size allowed by storm control on the *Switch* > *Storm Control* page and the *Edit Physical Port* page.
- Access control lists are now supported on the FSR-112D-POE model.
- Border Gateway Protocol (BGP) routing is now supported on the FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, and FS-448E-FPOE models.
- The following commands are now supported by the FS-148F, FS-148F-POE, and FS-148F-FPOE models:
  - `diagnose switch physical-ports qos-stats list`
  - `diagnose switch physical-ports qos-stats non-zero`
  - `diagnose switch physical-ports qos-stats set-qos-counter-revert`
  - `diagnose switch physical-ports qos-stats set-qos-counter-zero`
  - `diagnose switch physical-ports qos-rates list`
  - `diagnose switch physical-ports qos-rates non-zero`
- Setting the `switch-mgmt-mode` is no longer needed, so the `set switch-mgmt-mode` command has been removed from `config system global`.

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
   set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.2.0 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiSwitch Devices Managed by FortiOS Release Notes* for upgrade information. See https://docs.fortinet.com/document/fortiswitch/7.0.0/managed-switch-release-notes.

Product integration and support

FortiSwitchOS 7.2.0 support

The following table lists FortiSwitchOS 7.2.0 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.2.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
724558	A flash module failed and caused a complete network outage.
724813	The `set enforce-first-as {disable | enable}` command should have been placed under `config neighbor` and does not work in its current location (directly under `config router bgp`). There is no patch available for this issue.
741354	There is a segmentation fault when a packet is received for a deleted interface before the DHCP client module has removed that interface.
743749	When the network hub is disconnected and then reconnected, MAB sometimes does not work.
746584	An FS-448D cannot be access on an intermittent basis.
748177	When the network monitor is enabled, the MCLAG trunk becomes unstable.
748249	New CLI commands have been added under the `config switch security` command to control TCP and UDP ports.
752085	When the FortiSwitch unit sends the BPDU with the proposal bit on, it causes STP to be unsynchronized.
753630	MAB cannot be recovered after the daemon for 802.1x port-based authentication has crashed.
754232	Some FS-224D-FPOE switches have problems with checking the PSU GPIO.
759992	After the FortiSwitch unit is restarted, the memory usage increases, and users cannot access the FortiSwitch unit with the CLI or GUI.
760536	The SNMP trap for the power supply failing or being restored is using the wrong OID.
763264	Displaying the *Switch* > *Port* > *Physical* page or the dashboard causes high CPU usage.
763953	After the LDAP authentication succeeds, there is a “wrong username and password” error.
769733	The getnext query needs to be supported for OID .0/0.0.
771767	The switch cannot be accessed if the trusted host is not using /32.
787797	The FortiSwitch unit does not allow VTP traffic between Cisco switches.
796030	There is no response when SNMP polls a loopback interface.

Common vulnerabilities and exposures

FortiSwitchOS 7.2.0 is no longer vulnerable to the following CVEs:

- CWE-190
- CWE-347
- CWE-352
- CWE-610
- CWE-788

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The `get switch acl counters` commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 functionalities and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 functionalities, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
748210	After a third-party hub is disconnected and then reconnected, MAB sometimes does not work.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: • log-mac-event • DHCP snooping • LLDP-assigned VLANs • NAC
793821	A “Failed to send l2mac trap” message is reported if `log-mac-event` is enabled on one port without the SNMP-related information being configured.
795041	The VM debug report (*System* > *Debug Report*) is missing information for many CLI commands.
798357	When multiple VXLAN configurations use the same remote-ip value, the VXLAN tunnels do not update the underlying SVI IP address.
802786	Virtual IP addresses cannot be used in a FortiGate device to redirect the public IP address to the private IP address of the FortiSwitch unit.

www.fortinet.com